

(19)



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11)

EP 0 939 519 A1

(12)

EUROPEAN PATENT APPLICATION

(43) Date of publication:
01.09.1999 Bulletin 1999/35

(51) Int Cl.⁶: **H04L 12/28**, **H04L 12/22**,
H04L 29/06, **H04L 12/46**

(21) Application number: **99200388.9**

(22) Date of filing: **11.02.1999**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(72) Inventor: **Brockmann, Ronald Alexander**
3572 AX Utrecht (NL)

(74) Representative: **Van Breda, Jacobus**
Octrooibureau Los & Stigter B.V.,
P.O. Box 20052
1000 HB Amsterdam (NL)

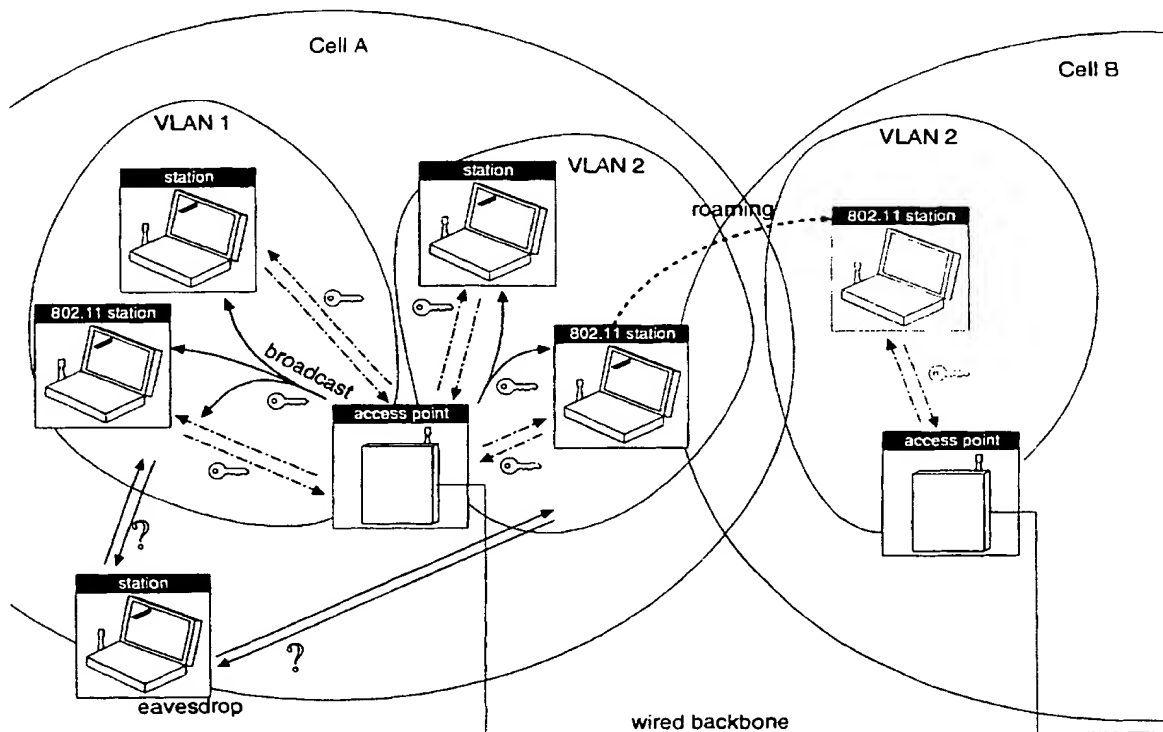
(30) Priority: **19.02.1998 NL 1008351**

(71) Applicant: **No Wires Needed B.V.**
3723 BS Bilthoven (NL)

(54) Data communication network

(57) The invention relates to a data communication network suitable for the exchange of data between computers, which network comprises at least one substantially wireless LAN (Local Area Network) and access points distributed over an area of coverage for linking

the computers comprised in the minimally one LAN, with the network. The minimally one wireless LAN is virtual and the data traffic with the computers belonging to that particular LAN is individualized by encoding the data exchanged between the computers and the access points by using for each LAN a unique key.



EP 0 939 519 A1

Description

[0001] The invention relates to a data communication network suitable for the exchange of data between computers, which network comprises at least one substantially wireless LAN (Local Area Network) and access points distributed over an area of coverage for linking the computers comprised in the minimally one LAN with the network.

[0002] Such a data communication network has been known in practice for years. The wireless local area network (LAN) comprised in such a data communication network is designed to provide a great degree of flexibility, mobility and to lower the otherwise necessary costs for infrastructure and control. Such a wireless LAN may include a laptop computer equipped for wireless communication. In order to provide the communication function, the network is equipped with so-called access points which are set up in the geographical area served by the wireless LAN. Usually an access point serves a small area called Cell, having a radius of between 10 and 100 metres. Therefore, for serving a somewhat extensive area of coverage, the application of several access points is required. Among themselves, these access points are linked by means of network techniques which are known as such, and which may or may not be wired, such as for example, the ethernet infrastructure.

[0003] The data communication network forming the object of the present invention, comprises at least one wireless local area network, and may otherwise be wired for linking with possibly further virtual local area networks, for example, in accordance with the IEEE 802.1Q standard for virtual LANs or, similarly, as known from W096/04734. When such a data communication network provides the possibility of applying several wireless local area networks, a problem arises that is intrinsic to the type of wireless communication. When computers from different local area networks operate in the same geographical area it is, in view of the fact that wireless communication takes place via the ether, very difficult to maintain the integrity of the data traffic in the respective local area networks according to the prior art.

[0004] There are various solutions to this problem. On the one hand, the number of access points may be enlarged in concurrence with the number of local area networks present in a certain area of coverage; however, this is very costly and with respect to the utilization of the available transmitter frequencies, very inefficient. Another solution is not to increase the number of access points, but to restrict the mobility of the computers in local area networks. However, instead of solving a problem it merely avoids a problem. Another possibility is to abandon the idea of the smaller local area networks and to equip the system as one integral network. This would indeed avoid the indicated problem, but would create problems relating to the security of the data traffic, and will produce an exponential increase of the control problem. Accordingly, the performance of the system will de-

teriorate because data which is destined for a limited number of computers, will be sent to every-one.

[0005] US 5.199.072 concerns wireless local area networks and means for restricting access within such networks. The wireless LAN according to this publication utilizes a control module to control communication with user modules that are linked with such devices as terminals, personal computers and similar equipment. Access to the wireless LAN is controlled by the control module and for each user module a unique identification number is employed, which information is stored in the memory of the control module. Prior to permitting network access the control module verifies the identification of the requesting user module. The users that are active in a certain geographical area, form part of a group sharing the same control module and when the mobile users are roaming, a transfer of the user concerned from one user group to the next is required, necessitating the assignment of a new password into the user module seeking access into the next user group. According to US 5.199.072 a particular user is, however, not able to roam from one area to the other whilst maintaining membership to one particular virtual LAN.

[0006] It is the object of the invention to provide a system in which the data communication network can be used whilst being able to encompass several wireless LANs, without unduly aggravating the control problem with respect to the data traffic in the system, and without requiring concessions with regard to the mobility of the various computer users who are part of a wireless LAN.

[0007] According to the invention the data communication network is therefore equipped such that the minimally one wireless LAN is virtual and that the data traffic with the computers belonging to that particular LAN is individualized by encoding the data exchanged between the computers and the access points by using for each LAN a unique key.

[0008] In one preferred embodiment therefore every computer is provided with its own unique key. In this manner point-to-point data links can be established between the various computers wirelessly encompassed in the network and the access points. To this end, data encoding techniques may be applied that are generally known from the literature. The only prerequisite being, that the keys applied are capable of distinguishing the individual data links between the respective computers and the access points. By providing said keys, the respective access points can be equipped such that they recognize to which virtual LAN or virtual LANs they belong and also, to which LAN the computers sending and/or receiving data to and from said access points, belong. The various keys may be determined beforehand for each LAN.

[0009] In one particular embodiment, however, it is advantageous that the data communication network is equipped to generate the unique key the moment that data traffic between one or more computers from a LAN and the network is established. This is advantageous

with regard to controllability.

[0010] One suitable embodiment endowed with the necessary guarantees regarding authentication of the data traffic, is characterized in that the generation of the unique key occurs with the public-key algorithm, which is known as such: see W. Diffie and M.E. Hellman, "New

Directions in Cryptography". IEEE Transactions on Information Theory, v.IT-22, n. 6, Nov 1976, pp. 644-654.

[0011] Advantageously, the access points are among themselves linked to wired network connections that are known as such. However, this is not a prerequisite: the network connections may also be wireless.

[0012] In order to restrict the load constituted by the data traffic in the data communication network according to the invention, it is desirable that every access point possesses a filter unit for deleting data destined for a computer belonging to a LAN other than the one present in the area of coverage of that particular access point, or which stems from a computer of a first LAN while being destined for a computer of a second LAN. In addition, this guarantees the virtual star structure of the network.

[0013] With a view to data traffic security it is desirable that the filter unit be equipped to delete from the data traffic predetermined types of data, for example, data that could be classified as infringing the security or integrity of a network or a part thereof. This may be of particular importance with regard to data exchange in a WINDOWS-NT environment.

[0014] To further serve the controllability of the system, every computer in a wireless LAN is provided with a device for rejecting messages sent by other computers. This procedure effectively provides a star structure between the various access points and the computers communicating with said access points.

[0015] It is further desirable that each computer be provided with one or more additional keys for encoding and decoding the data traffic destined for a group of computers, or for all computers in the same virtual LAN. In addition to the point-to-point data message communication on an individual basis, the virtual LAN would then also provide the possibility of multipoint message communication and broadcast message communication.

[0016] Application of the invention is possible by using the standard IEEE 802.11 technology for wireless local area networks. By applying the invention, the respective wireless virtual local area networks are distinguished and separated from each other, without the risk of data traffic arriving at any other than the intended destination. The invention enables the computer users within the various local area networks to move about freely within the area served by the various access points.

[0017] The invention will now be further elucidated with reference to a single drawing which schematically shows the data communication network according to the invention.

[0018] The data communication network shown is

suitable for data exchange between computers, each of which is indicated by the term "station". The data communication network shown comprises, at least in the portion shown, two virtual local area networks indicated by VLAN 1 and VLAN 2. The virtual local area networks VLAN 1 and VLAN 2 are linked with the network via data traffic through the ether, taking place with the aid of an access point, indicated as such in the figure. According to the invention, the data traffic between such an access point and the computers "station" is encoded by means of a key code which, in the case illustrated, is unique for each computer, whereby an individualized link is provided between each computer "station" and the respective access point. Another possibility is to apply such a unique key code only per LAN, so that all computers of that particular LAN are able to participate in the data traffic. The unique key is, for example, determined for each LAN or computer beforehand. Another possibility is to postpone the determination of the unique key until the moment that data traffic between one or more computers from a LAN and the network is imminent. Generation may then be effected by means of a public-key algorithm. Such public-key algorithms are known to the expert and require no further explanation.

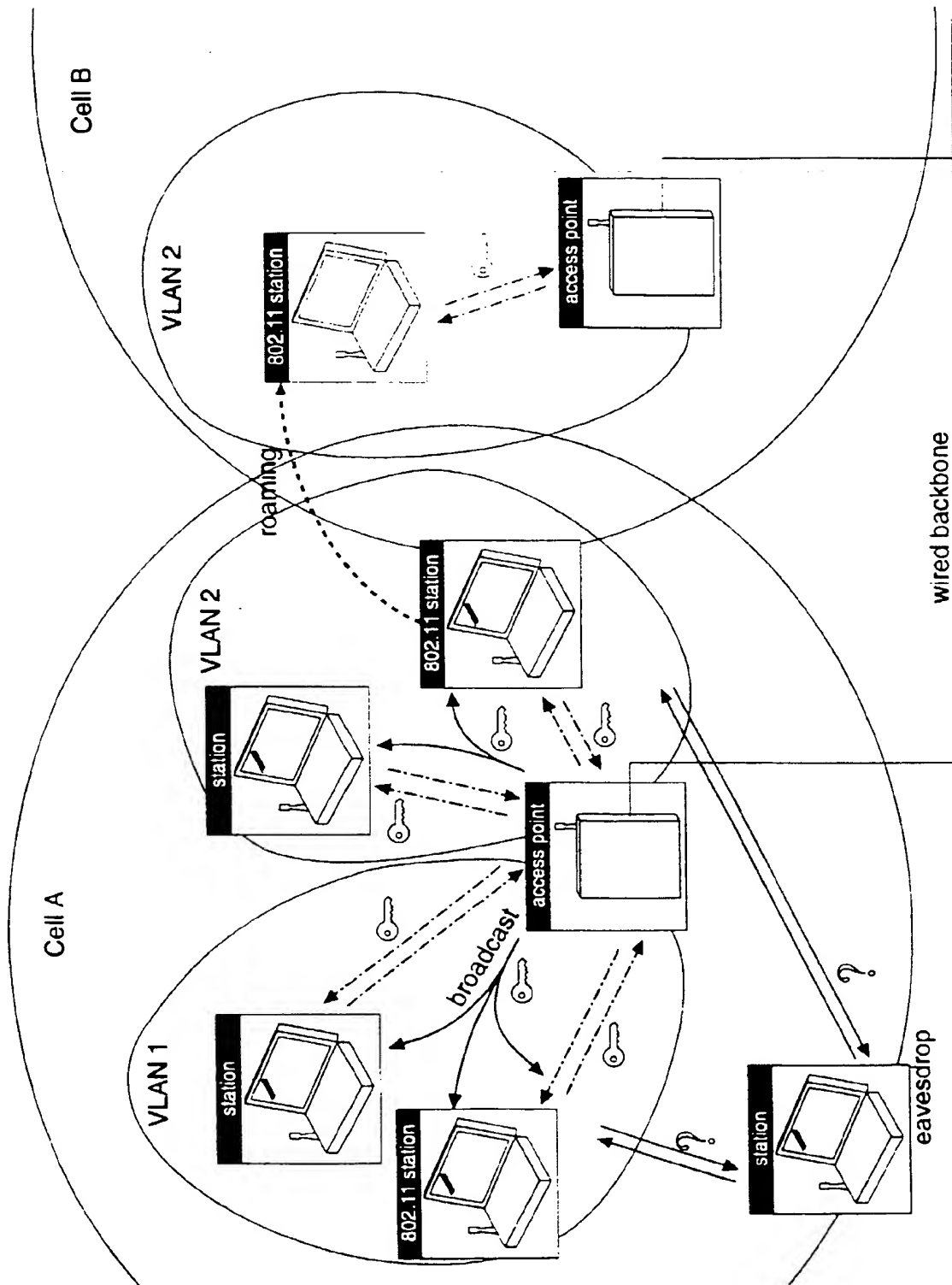
[0019] The figure shows further that the respective access points are interlinked by means of wired network links which are known as such, and called "wired backbone". To make effective use of the data communication network without overloading by excessive data traffic, each access point is provided with a filter unit for deleting any data destined for a computer of LAN VLAN 1 or VLAN 2 respectively, other than the one present in the respective area of coverage (Cell A or Cell B) of that particular access point. The filter unit is also equipped to delete data sent from a first LAN and destined for a computer of a second LAN. The result is a logical separation of the VLANs. Said filter unit can also delete specific types of data. Furthermore, every computer "station" is equipped with an element for rejecting data sent by another computer "station". In this manner the data network acquires a star structure.

[0020] Thanks to the virtual and wireless character of the local area networks applied in the network according to the invention, a computer station forming part of local area network VLAN 2, may be moved from the one area of coverage Cell A to an area of coverage Cell B, served by another access point, without losing the integrity of a local area network. Thus the advantage of the invention is that, despite the use of wireless computers "station" together with virtual local area networks, the advantages associated with said latter technique, namely improved controllability of the data traffic in the data communication network is realized without conceding anything to the mobility of the computers used in the network. Thanks to the filter units provided in the various access points forming part of the network, the speed of the data traffic in this network, and the logical separation of the LANs is guaranteed.

Claims

1. A data communication network suitable for the exchange of data between computers, which network comprises at least one substantially wireless LAN (Local Area Network) and access points distributed over an area of coverage for linking the computers comprised in the minimally one LAN, with the network, **characterized** in that the minimally one wireless LAN is virtual and that the data traffic with the computers belonging to that particular LAN is individualized by encoding the data exchanged between the computers and the access points by using for each LAN a unique key. 5 10 15
2. A data communication network according to claim 1, **characterized** in that every computer is provided with its own unique key. 20
3. A data communication network according to claim 1 or 2, **characterized** in that the data communication network is equipped to generate the unique key the moment that data traffic between one or more computers from a LAN and the network is established. 25
4. A data communication network according to claim 3, **characterized** in that the generation of the unique key occurs with a public-key algorithm. 30
5. A data communication network according to one of the claims 1-4, **characterized** in that among themselves, the access points are linked by means of wired network links. 35
6. A data communication network according to one of the claims 1-5, **characterized** in that every access point possesses a filter unit for deleting data destined for a computer belonging to a LAN other than the one present in the area of coverage of that particular access point, or which stems from a computer of a first LAN while being destined for a computer of a second LAN. 40
7. A data communication network according to claim 6, **characterized** in that the filter unit is equipped to delete from the data traffic predetermined types of data. 45
8. A data communication network according to one of the claims 1-7, **characterized** in that every computer in a wireless LAN is provided with a device for rejecting messages sent by other computers. 50
9. A data communication network according to one of the preceding claims, **characterized** in that each computer is provided with one or more additional keys for encoding and decoding the data traffic des-

tined for a group of computers, or for all computers in the same virtual LAN.





European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 99 20 0388

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X	US 5 199 072 A (WHITE RICHARD E ET AL) 30 March 1993	1,5,8,9	H04L12/28 H04L12/22 H04L29/06 H04L12/46
Y	* abstract * * column 1, line 7 - column 2, line 43 * * column 4, line 28 - column 5, line 1 * * figures 1,2 *	2,3,6	
Y	US 5 309 516 A (TAKARAGI KAZUO ET AL) 3 May 1994	2,3	
A	* abstract * * column 1, line 23-39 * * column 2, line 56 - column 4, line 17 * * column 6, line 45 - column 7, line 19 * * column 10, line 28-38 * * column 10, line 64 - column 12, line 25 *	4	
Y	WO 96 04734 A (IBM ; IBM UK (GB)) 15 February 1996	6	
A	* abstract * * page 1, line 25-28 * * page 2, line 12 - page 3, line 7 * * page 3, line 33 - page 5, line 43 *	7,8	TECHNICAL FIELDS SEARCHED (Int.Cl.6) H04L
A	WO 95 12942 A (NORAND CORP) 11 May 1995 * abstract * * page 4, line 1 - page 5, line 3 * * page 51, line 25-47 * * figures 3,5-7 *	1	
The present search report has been drawn up for all claims			
Place of search THE HAGUE		Date of completion of the search 26 May 1999	Examiner Lievens, K
CATEGORY OF CITED DOCUMENTS X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document		T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document	

EPO FORM 1503 03.82 (IP/C01)

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 99 20 0388

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

26-05-1999

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5199072 A	30-03-1993	NONE	
US 5309516 A	03-05-1994	JP 5347616 A	27-12-1993
		JP 4213242 A	04-08-1992
		US 5351294 A	27-09-1994
		US 5218638 A	08-06-1993
WO 9604734 A	15-02-1996	CA 2129197 A	30-01-1996
		AT 164481 T	15-04-1998
		CZ 9603749 A	16-04-1997
		DE 69501896 D	30-04-1998
		DE 69501896 T	22-10-1998
		EP 0772931 A	14-05-1997
		ES 2114326 T	16-05-1998
		HU 76242 A	28-07-1997
		JP 8065303 A	08-03-1996
		PL 318320 A	09-06-1997
WO 9512942 A	11-05-1995	AU 679593 B	03-07-1997
		AU 1089595 A	23-05-1995
		CA 2175700 A	11-05-1995
		EP 0740873 A	06-11-1996
		US 5748619 A	05-05-1998

EPO FORM P0159

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

THIS PAGE BLANK (USPTO)